

8



The Crown Prosecution Service

[Home](#) » [Professionals](#) » [Legal Guidance](#) » [Disclosure and Covert Law Enforcement](#) » [Covert Surveillance](#)

Covert Surveillance

- [Principle](#) |
- [General application of ECHR](#) | [CPS Advice to Police](#) | [Guidance](#) |
- [The Law](#) | [Role of the Surveillance Commissioner](#) | [Regulation of Investigatory Powers Act 2000 - "intrusive" and "directed" surveillance](#) | [Authorisations under the Police Act 1997](#) | [Recent Caselaw concerning covert listening devices](#) | [Authorisations under RIPA](#) | [Directed Surveillance](#) | [Circumstances where the Chief Constable must authorise](#) | [Intrusive Surveillance](#) | [Surveillance Commissioners](#) | [Other Surveillance](#) | [Guidance on Prosecutions](#) | [Internal Referral Requirements](#) | [Advice to the Police](#) | [Validity of Authorisations](#) | [Viewing the authorisation documentation](#) | [Requirement for statement from the Authorising Officer](#) | [Surveillance Records](#) | [Security of Surveillance Logs](#) | [Surveillance Logs - disclosure issues](#) | [Revealing the Location of an Observation Point](#) | [Surveillance Equipment - Video and Audio Tapes](#) | [Useful Links](#) |

Quick Links

- [Code for Crown Prosecutors](#)
- [History of the CPS](#)
- [Factsheets](#)
- [Contact Us](#)

Principle

As criminals become more sophisticated in their methods, so the methods of detecting and investigating crime must become more sophisticated. In recent years there has been a significant shift in the nature of policing with a greater emphasis on intelligence driven, proactive policing. In addition, the technological means whereby the police can gather information covertly have also advanced rapidly.

The use of covert techniques have had to be reassessed in the light of the likely impact of Articles 6 and 8 of the European Convention on Human Rights

** Use Police Act, 1997 - Part III
sects. 97 - 108
* RIPA, 2000.
check.*

(ECHR).

[Top of page](#)

General application of ECHR

Article 8 guarantees a right to private and family life and correspondence. The means by which an individual's privacy can be invaded are developing rapidly. Two conflicting public interests must be balanced - the public interest in the prevention of crime and the need for constraints on state power to intrude into individual life. But the rights of privacy (Article 8) and to a fair trial (Article 6) are not absolute rights and the European Court has consistently stated that they must be weighed against the restrictions imposed on those rights to protect other members of society.

Covert police operations by their very nature involve some degree of invasion of the right to privacy. It is anticipated that where breaches of Article 8 can be established, defendants will argue that the deployment of covert techniques and/or the reliance in evidence on the product of such techniques deprives them of the right to a fair trial guaranteed by Article 6.

Alternatively, defendants may seek to argue that by virtue of the breach, evidence gathered as a result of the deployment of such techniques should be subject to the discretionary exclusion of evidence in section 78 of PACE.

The House of Lords has made it clear that the courts are entitled to take account of alleged breaches of Article 8 in determining how to exercise the section 78 discretion - **R-v-Sultan Khan [1997] AC 558**.

[Top of page](#)

CPS Advice to Police

The growth of covert policing and the impact of ECHR will inevitably lead to an increase in cases where the police seek advice from The CPS in the investigative stage of an operation. CPS advice should be limited to the likely evidential implications of a proposed course of action. Whether specific covert techniques should be deployed in a particular case is an operational decision for the police.

There must be no question of The CPS approving,

authorising or condoning the commission of any criminal offence in a particular case. Prosecutors should not advise on ancillary legal issues such as liability for trespass or damage caused whilst installing covert devices.

[Top of page](#)

Guidance

The Law

The use of covert surveillance techniques is regulated by two pieces of legislation. For details of the authorisation required **<refer to Authorisations under the Police Act 1997, below in this section>** and **<Authorisations under RIPA below in this section>**

Police Act 1997 - surveillance involving "interference with property"

Part III of the Police Act 1997 (PA) deals with the procedure for the authorisation of surveillance which involves an "interference with property" or wireless telegraphy.

<http://www.hmsso.gov.uk/acts/acts1997/1997050.htm>

Part III provides that no entry on or interference with property shall be unlawful if it is authorised under the Act. It provides a procedure for obtaining authorisation for police action that involves an entry on or interference with property. The Act also provides for the appointment of a Chief Commissioner and a number of Commissioners to oversee the authorisation process and to give prior approval for the more intrusive forms of intrusive surveillance involving dwelling houses or office premises.

[Top of page](#)

Role of the Surveillance Commissioner

Where the authorising officer believes that any of the property specified in the authorisation is used wholly or mainly as a dwelling or as a bedroom in an hotel, or constitutes office premises or the action authorised is likely to result in any person acquiring knowledge of matters subject to legal privilege, confidential personal information, or confidential journalistic information, he or she may authorise the operation but the

authorisation does not take effect until a Commissioner has notified the authorising officer that the authorisation has been approved. There is an exemption for prior approval in cases of urgency. **<See Intrusive Surveillance, below in this section>**

You may be asked to advise the police as to whether a proposed surveillance operation requires prior approval under the Act. The law on trespass will provide guidance on whether prior approval is required. *De minimis* trespasses, for example, by an officer jumping behind a hedge to avoid being seen, are unlikely to require prior approval. Prior approval under this Act is also unlikely to be required for undercover officers who enter dwellings or hotels, for example, in a drugs purchase operation. This is on the basis that the officer has been given a licence to enter those premises by the owner, and this licence is not vitiated by the true motive for the officer's presence.

A trespass will not occur, and so the prior approval of a Commissioner will not be required, if there is consent to enter on or interfere with property. The person who can give a valid consent will be the one against whom a trespass would otherwise be committed, i.e. the person who could maintain an action for trespass if the operation was carried out without consent. Such conduct would, however, require authorisation under RIPA.

[Top of page](#)

Regulation of Investigatory Powers Act 2000 - "intrusive" and "directed" surveillance

Part II of the Regulation of Investigatory Powers Act 2000 (RIPA) regulates other forms of covert surveillance referred in the Act as "intrusive surveillance" and "directed surveillance". < <http://www.legislation.hmso.gov.uk/> >

All forms of covert surveillance are now also supported by a Code of Practice issued pursuant to section 71 RIPA .

There is no definition of "interference with property" contained within the Police Act 1997. The law on trespass will provide guidance on whether prior approval is required.

Definitions of covert, directed and intrusive surveillance are at s26 RIPA <
<http://www.legislation.hmso.gov.uk/acts/acts2000/00023--d.htm#26> >

For guidance as to the caselaw on "eavesdropping", see **(Archbold 15-501)**

[Top of page](#)

Authorisations under the Police Act 1997.

Authorisation for surveillance to which the Police Act applies may be given by a Chief Constable, but only when the application is made by a member of his or her force and the action is to be taken within his or her force area. Grounds for authorisation are set out in s93 Police Act. <

<http://www.hmso.gov.uk/acts/acts1997/97050--j.htm#93> >

The power to grant authorisation may be delegated in cases where it is not reasonably practicable for an authorising officer to consider the application.

[Top of page](#)

Recent Caselaw concerning covert listening devices

In **P.G. and J.H. -v- UK (Application no.44787/98) (The Times October 19, 2001)(Lawtel)** the European Court of Human Rights considered a number of issues involving covert listening devices and non-disclosure of unused material. This case was prior to the Regulation of Investigatory Powers Act 2000 becoming law.

The court held that the use of a covert listening device at a defendant's flat was a violation of Article 8 as this had not been properly authorised in accordance with the law at any time. The court held that the use of listening devices in the police station did not comply with the requirement of lawfulness because at the relevant time there existed no statutory system to regulate the use by the police of covert listening devices on their premises. The court noted that the Regulation of Investigatory Powers Act 2000 (part II) contains provisions regulating this.

However, having regard to **Khan -v- UK (2000)**, the court confirmed that there was not a violation of Article 6(1) as the use of the taped evidence and voice samples at the trial did not conflict with the requirements of fairness.

The court also held that there had not been a breach of the applicants' rights in respect of the non-disclosure to the defence of a number of documents which had been the subject of a PII application. In considering **Jasper -v- UK (2000) and Fitt -v- UK (2000)** the court stated that "the entitlement to disclosure of relevant evidence is not an absolute right". On the facts of this particular case, where the defence had been kept informed and had been permitted to make submissions, the court considered that, "the decision making procedure complied with the requirements of adversarial proceedings and equality of arms and incorporated adequate safeguards to protect the interests of the accused."

Where authorisations have been given, renewed, or cancelled, the authorising officer must as soon as reasonably practicable notify a Commissioner appointed under the Act.

In some circumstances set out at section 97 Police Act , <

<http://www.hmso.gov.uk/acts/acts1997/97050-k.htm#97> > the authorising officer may authorise the operation but the authorisation does not take effect until a Commissioner has notified the authorising officer that the authorisation has been approved. There is an exemption for prior approval in cases of urgency.

Such conduct would, however, require authorisation under RIPA - **<refer to Authorisations under RIPA below in this section>**.

Authorisations will normally last for three months but can be renewed before they cease to have effect provided that the criteria for authorisation are still satisfied. Authorisations granted by designated deputies and all oral authorisations granted in cases of urgency are valid for only 72 hours. An authorisation must be cancelled when the action authorised is no longer necessary.

[Top of page](#)

Authorisations under RIPA

[Top of page](#)

Directed Surveillance

Covert surveillance activity which does not involve an interference with property and so falls outside the scope of the 1997 Act will be authorised and conducted in accordance with RIPA.

RIPA draws a distinction between 'directed' surveillance and 'intrusive' surveillance.

Directed surveillance is defined as covert surveillance that is not intrusive and is undertaken for the purposes of a specific investigation in such a manner as is likely to result in the obtaining of private information about a person, (whether or not specifically identified for the purpose of the investigation or operation).

Authorisation for directed surveillance may be granted by a superintendent or, in cases of urgency where no superintendent is available, by an inspector. Grounds for authorisation are set out in section 28 RIPA.
<http://www.legislation.hmso.gov.uk/acts/acts2000/00023--d.htm#28#>

[Top of page](#)

Circumstances where the Chief Constable must authorise

The authorisation must be granted by the Chief Constable where the likely consequence of the directed surveillance would be for any person to acquire knowledge of confidential material.

Authorisations must be in writing save in urgent cases in which event a superintendent may grant them orally. Written authorisations last for three months. Oral authorisations and authorisations granted by an inspector in urgent cases last for 72 hours. Authorisations can be renewed before they cease to have effect provided that the criteria for authorisation are still satisfied. An authorisation must be cancelled when the action authorised is no longer necessary.

[Top of page](#)

Intrusive Surveillance

Intrusive surveillance is defined as covert surveillance which is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle, or is carried out by means of a surveillance device.

The Chief Constable must grant authorisation for intrusive surveillance although there is provision for authorisation, in cases of urgency, by an Assistant Chief Constable. Grounds for authorisation are set out in section 32 RIPA.

<http://www.legislation.hmso.gov.uk/acts/acts2000/00023--d.htm#32>

In addition to authorisation by the authorising officer, the grant (or renewal) of an authorisation for intrusive surveillance must be approved by a Surveillance Commissioner unless the case is one of urgency. Save for urgent cases, authorisations will not take effect until the Surveillance Commissioner has given written notice of approval to the authorising officer. **<See Role of the Surveillance Commissioner, above in this section>**

As in the case of directed surveillance, authorisations last for three months. Urgent authorisations granted by an Assistant Chief Constable last for 72 hours. Authorisations can be renewed before they cease to have effect provided that the criteria for authorisation are still satisfied.

[Top of page](#)

Surveillance Commissioners.

The Surveillance Commissioner must quash an authorisation (or renewal) if s/he is not satisfied that the criteria are satisfied or, in urgent cases, s/he is not satisfied that there were reasonable grounds for believing the case to be one of urgency. In addition, the Surveillance Commissioner must cancel an authorisation if satisfied at any time that an authorisation is in force that the criteria are no longer satisfied. The authorising officer is also under a duty to cancel an authorisation (or renewal) if satisfied that the criteria are no longer met.

There is a right of appeal to the Chief Surveillance Commissioner against the decision of a Surveillance Commissioner to refuse to approve an authorisation (or

renewal) or to quash or cancel an authorisation (or renewal).

[Top of page](#)

Other Surveillance.

Certain types of surveillance are outside the statutory regime and will require authorisation in accordance with local force orders.

[Top of page](#)

Guidance on Prosecutions

[Top of page](#)

Internal Referral Requirements

The use of covert surveillance techniques often raises difficult and sensitive issues. It is impracticable to require that all cases involving covert surveillance be handled at a particular level. Nevertheless, managers will need to ensure that suitably experienced lawyers oversee such cases. Early consultation with the police will usually be appropriate to identify difficult disclosure issues. In extreme cases, for example, where it is considered necessary to abandon a prosecution rather than reveal the identity of an observation post, it is essential that these issues are addressed at an early stage.

[Top of page](#)

Advice to the Police

You may be asked to advise the police as to whether a proposed surveillance operation requires prior approval under the Police Act, 1997. The law on trespass will provide guidance on whether prior approval is required. *De minimis* trespasses, for example, by an officer jumping behind a hedge to avoid being seen, are unlikely to require prior approval. Prior approval under the PA is also unlikely to be required for undercover officers who enter dwellings or hotels, for example, in a drugs purchase operation. This is on the basis that the officer has been given a licence to enter those premises by their owner, and this licence is not vitiated by the true motive for the officer's presence.

A trespass will not occur, and so the prior approval of a

Commissioner will not be required, if there is consent to enter on or interfere with property. The person who can give a valid consent will be the one against whom a trespass would otherwise be committed, ie. the person who could maintain an action for trespass if the operation was carried out without consent.

[Top of page](#)

Validity of Authorisations

Where a surveillance operation has not been properly authorised in accordance with the statutory regime, the defence may argue that the surveillance amounts to a breach of Article 8 of the ECHR and that the surveillance evidence should be excluded, either by virtue of the court's discretion under section 78 PACE, or on the basis that it infringes the defendant's right to a fair trial under Article 6.

In either instance, the court will have to consider the impact of the admission of the evidence on the fairness of the proceedings as a whole. Although the decisions of a Commissioner cannot be scrutinised in a court, the police can expect to be closely challenged to ensure that all procedural requirements relating to the authorisation have been satisfied. This may involve senior police officers having to give evidence. It is essential, therefore, that prosecutors have a good working knowledge of Part III of the 1997 Act, and Part II of RIPA.

When reviewing cases in which the prosecution seeks to adduce evidence gathered as a result of a surveillance operation, you will need to consider what type of surveillance was deployed. You will need to be satisfied that the necessary level of authorisation was obtained.

[Top of page](#)

Viewing the authorisation documentation

This will necessitate you viewing the authorisation documentation which is likely to contain material which will identify sources of intelligence. If there is any question of this documentation being disclosed you will need to consider disclosure of edited copies. It may be necessary to seek a ruling from the court in this regard. **<Refer to Disclosure of Unused Material in**

this guidance>[Top of page](#)

Requirement for statement from the Authorising Officer

Once it is known that the validity of a surveillance authorisation is to be an issue in the case, it will be necessary for the senior authorising officer to make a witness statement. In view of the large number of such authorisations, it has been agreed with the police that authorising officers will only provide statements on request. The police have been reminded of the need to ensure that the authorisation documentation contains sufficient detail to enable authorising officers to demonstrate, in their witness' statements, that the appropriate criteria were applied in the course of the decision making process.

Where a statement is requested from the relevant authorising officer it is suggested that it should cover the following:

- The grounds for granting the authorisation
- The date on which the authorisation was given
- The date on which the authorisation was submitted to a Commissioner (where appropriate)
- What actions were authorised
- That prior approval had been granted by a Commissioner (where appropriate)
- The grounds for granting oral authorisation (where appropriate)

If a person other than an authorising officer gave the authorisation, the person who granted the authorisation should make the statement. In addition to the matters set out above, the statement should set out the reason why delegated powers were used.

[Top of page](#)

Surveillance Records

The nature of surveillance requires that any necessary record keeping is carried out covertly. Records or logs created by officers involved in the surveillance are no more than memory refreshing documents which may be used by the officers when giving evidence, subject

to the consent of the court. However, all records or logs must be made on the understanding that they may be produced in evidence, or made the subject of an order for disclosure to the defence.

The police should notify The CPS of any case where surveillance logs exist. Details of the surveillance logs will usually appear on Form MG6C (schedule of unused material). Only in rare cases, where the surveillance evidence is not relied upon as part of the prosecution case and it is contended that it is not in the public interest to disclose the fact that there has been a surveillance operation, will it be appropriate to include such details on Form MG6D (schedule of sensitive unused material). In cases where no notification is made to CPS, but it appears that police evidence of observation may have resulted in the keeping of such a log, you should ask at the earliest opportunity if a log exists.

[Top of page](#)

Security of Surveillance Logs

The security of surveillance logs is considered by the police to be of paramount importance. They will not be copied to The CPS as a matter of routine. They must be made available, however, for detailed inspection and if copies are required for any purpose (for example, placing before a judge on an application to withhold material) you should make the request of the senior police officer in the case.

[Top of page](#)

Surveillance Logs - disclosure issues

The police may put forward a number of reasons why surveillance logs which would otherwise fall to be disclosed should be withheld from the defence. It may be that disclosure of the documents would reveal the location of the observation point or the identity of other targets of the operation who are still under investigation. In such cases it may be possible to edit passages from the logs which it is considered should be withheld in the public interest. < **R efer to Disclosure of Unused Material section elsewhere in this guidance**>

[Top of page](#)

Revealing the Location of an Observation Point

Where the prosecution relies upon surveillance evidence, the defence may wish to ascertain the precise location of the point from which the surveillance was conducted. There may be no difficulty with this in some cases. In other cases, however, members of the public may have co-operated with the police by permitting their premises to be used for surveillance on the understanding that details of the premises or other information which might lead to the premises being identified would not be disclosed. The well-established principle that information about informants should not be disclosed unless non-disclosure would result in a miscarriage of justice has been extended to protect the identity of premises used for surveillance.

The Court of Appeal has laid down minimum evidential standards which must be satisfied. (**Archbold, 12.37**) (**R.v. Johnson [1998] 1 WLR 1377**)

You will need to be alert to ensure that these procedures have been followed and where have not been you will need to advise the police that it is likely that the court will order that the location of the observation point be revealed. In extreme cases, it may be necessary to abandon the prosecution to protect individuals who have assisted the police in this way.

The principle is based on the protection of the owner or occupier of the premises used and not on the identity of the observation post itself. In **R.v. Brown and Daley [1987] 87 Cr.App.R 52**, the Court of Appeal ruled that the trial judge had been wrong to exclude evidence of the make, model and colour of a police vehicle used for a surveillance operation. However, the court did say that, "with the advent of sophisticated methods of investigation, there may be cases where..public interest immunity may be successfully invoked in criminal proceedings to justify the exclusion of evidence as to police techniques and methods."

[Top of page](#)

Surveillance Equipment - Video and Audio Tapes

In addition to conventional surveillance evidence, the police may wish to rely upon evidence gathered by the use of surveillance equipment. This will usually consist of video recordings made from a surveillance point or audio recordings obtained from a covertly placed recording device.

There will be cases where the police contend that copies of surveillance videos, video stills or conventional photographs taken from an observation point should not be supplied to the defence on the basis that detailed study by the defence might enable them to identify the observation post. Even where such a position can be sustained, it will be necessary to allow the defence access to view or listen to tapes.

Where tapes are to be released to the defence, you should consider seeking a written undertaking from the defence solicitor that they will not be copied or released in to the custody of the defendant.

[Top of page](#)

Useful Links

<http://www.hmso.gov.uk/acts/acts1997/1997050.htm>

<http://www.homeoffice.gov.uk/ripa/ripact.htm>

<http://www.homeoffice.gov.uk/ripa/ripadcp.htm>

<http://www.legislation.hmso.gov.uk/acts/acts2000/00023--d.htm#26>

<http://www.hmso.gov.uk/acts/acts1997/97050--j.htm#93>

<http://www.hmso.gov.uk/acts/acts1997/97050--k.htm#97>

<refer to RIPA guidance in this chapter>.

<http://www.legislation.hmso.gov.uk/acts/acts2000/00023--d.htm#28>

<refer to disclosure section in this guidance>

(Archbold, 12.37)

v1.1

[Top of page](#)

(9)

Note of meeting with [REDACTED], Office of the Attorney General and [REDACTED], Office of the DPP on 16 May, 2008 to discuss aspects of the proposed Covert Surveillance Bill.

I outlined the scope of the proposals we had in mind which met with broad approval. [REDACTED] said that the definition of "covert surveillance" was crucial to the whole project and offered some advice in that regard, which has been followed in the draft heads. There was general agreement that there was no need to include a specific provision in the Bill providing that information or material obtained through the use of covert surveillance may be used by the prosecution during the course of a criminal trial. It is well accepted that this is the case and it is a regular feature in dissident republican cases that Garda observational evidence about tracking persons in public, meetings and general movements is produced. Similarly in the recent case involving potential arms imports by certain Limerick gang factions, information of this nature arising not just from Garda sources, but also the UK police was introduced. However, it should be noted that the case was not fought as the defendants pleaded guilty.

However, the provisions in the Bill will be wider in that they will covert surveillance in private dwellings, hotels and other places generally and may involve the use of not only secret filming but conversations.


[REDACTED] noted that in gangland cases generally, the use of information obtained through covert operations will continue to be of crucial probative importance given that ordinary civilian witnesses frequently refuse to give direct evidence out of fear.

As to the question of disclosure, it was generally agreed that the common law was sufficiently well developed here on the subject of the obligation on the prosecution to give the defence any information which could be of an exculpatory nature, even evidence that might be damaging to the prosecution case. Any provision in the Bill providing for a mechanism to allow the prosecution to withhold disclosure of other evidence on the grounds that for example, revealing it could compromise Garda operational capacity; or be contrary to the wider public interest; or affect the security of the State would have to be expressed as being without prejudice to existing rules in this area.

Both [REDACTED] and [REDACTED] thought that it might not be strictly necessary to provide for a statutory exception for non disclosure on the basis that again, the matter would, in the course of normal practice, automatically be raised with trial Judge for a decision. They cautioned that in this jurisdiction the norm is for applications to exclude evidence to be construed very strictly against the prosecution. Most are resolved in favour of the defence except in the most exceptional of cases, say, relating to preserving the identity of a crucial State witness.

Nevertheless, they agreed that once the provisions relating to the new rules become law, defence applications for details on the use of surveillance, methods, etc., will become the norm. On balance they suggested that for the purposes of further discussion, a draft head should be included on the point. It is possible that the AG's Office might consult counsel on the issue - Mr. [REDACTED] was named

as a possible option in this regard. It was agreed that I should prepare the draft Heads accordingly for consideration at another meeting.


16 May, 2008.

9/3

[REDACTED] /JELR/JSECTOR
12/05/2008 16:02

To [REDACTED]@dppireland.ie
cc
bcc
Subject Meeting on covert surveillance issues

Just to follow up on my earlier 'phone call: I wrote to the Deputy Director on 2 May last concerning draft legislation being prepared here on the use of covert surveillance apparatus by the Garda Síochána. At the moment, this is an area which is not regulated by law. Thus, the activities of the garda Síochána are in breach of the ECHR.

In the course of the work on the draft legislation, the question of the actual use as evidence by the prosecution in court of any information obtained gained by such surveillance has arisen. A policy decision has been taken to include such a provision in the legislation together with statutory rules in relation to what may or may not be disclosed to the defence in such cases. The purpose of the rules on non-disclosure is to protect Garda operational capability in such matters.

Arising out of the meeting here between the Secretary General and the Deputy Garda Commissioner (Operations), we thought it would be useful in the first instance to explore the disclosure issue in detail with both [REDACTED] of the AG's Office and the Deputy Director. [REDACTED] has suggested a meeting in his office at 9.30 am on Friday next. It would be very useful if the Deputy Director could attend or send an alternative. This is for the purpose of getting a practical prosecutorial view on the issue and to take account of any particular views that the DPP's Office may have before presenting formal proposals to the Government.

Regards

[REDACTED]

Criminal Law Reform Division

9C

Draft legislative provisions on covert surveillance and the possible use of information gained thereby in evidence in criminal trials:

Steering Note for meeting on 2 May, 2008.

General background:

Specific recommendations made by both the previous and present Commissioner in this area and also in relation to interception issues, have been considered and developed into preliminary draft legislative proposals. This work is against the background of concerns over possible challenges under the 2003 ECHR Act on the basis that the Strasbourg Court has already ruled that covert surveillance operations breach the Convention (Articles 6 and 8 – right to fair trial and privacy respectively, in the latter case - unless they are regulated by law). Phone intercepts have been so regulated under the Ministerial Warrant procedure in the 1993 Act.

These proposals also have taken account of recommendations made by the Law Reform Commission and legislation in the UK, notably the Criminal Procedure and Investigations Act 1996, the Police Act, 1997, the Regulation of Investigatory Powers Act, 2000 and the Criminal Justice Act, 2003. The Labour Party Private Member's Garda Síochána (Powers of Surveillance) Bill, published in November, 2007 has also been considered.

The proposals deal only with the legal rules governing the issuing of Judicial and Garda authorisations for covert surveillance and particular technical aspects related to the interception issue (e.g., the closing down of particular cellular areas). The question of the possible use of information obtained as a result of covert surveillance operations in criminal trials was not considered. In the light of new thinking in that regard, it will be necessary to consider this matter in some detail. Also, against the background of a Report by the UK Privy Council published on 30 January, 2008, on the question of the use of intercept material as evidence, it would be as well perhaps to consider this aspect of the matter also.

Some General principles as to issues raised:

There is an overriding imperative to safeguard national security. It is a basic function of the State to protect the public from threats, such as international terrorism and criminality.

Interception and covert surveillance provides both tactical and strategic information for the Garda Síochána. By these means, real time intelligence is provided on the plans and actions of terrorists, criminals and others which allows the Gardaí to disrupt plans and frustrate actions. It provides evidence against the perpetrators and facilitates arrests. It can also reveal new targets as well as the significance, long term plans, international connections and modus operandi of these groups and individuals. Under the Constitution and Articles 6 (right to a fair trial) of the ECHR, trials in these cases must be and be seen to be procedurally fair.

Any intercept material or information obtained through covert surveillance would have to be compatible with these provisions before its use as evidence would be permissible.

The issue of disclosure to the defence:

The normal common law rules of disclosure as underpinned by the “equality of arms principle” in order to mitigate any possible unfairness to the accused, would apply – most likely in the matter being decided by the trial judge. This could result in material being examined and that which may support the defence case or undermine the prosecution case, disclosed. Ultimately, the ability to secure a fair trial in any particular case and the need to safeguard national security may not be reconcilable. In that case the only remaining option for the State, if its security procedures and operations relating to sensitive techniques and capabilities may be opened up to public scrutiny, will be not to prosecute or, if proceedings have already begun, to withdraw the case.

In essence, fairness requires that any material held by the prosecution which weakens its case or strengthens that of the defence, if not relied on as part of its formal case against the accused, should be disclosed to the defence.

However, in support of the system of statutory disclosure as developed in the UK, the Court of Human Rights has stated that “the entitlement to disclosure of relevant evidence is not an absolute right”. (*Jasper and Fitt v the UK* (2000)). This is in the context of provisions which allow exculpatory material to be withheld on the basis of a system of Public Interest Immunity (PII) based on ex parte hearings if -

- there is an important countervailing public interest focussed on the real damage that could be caused to that interest,
- non-disclosure is strictly necessary to protect that interest, and
- any difficulty caused to the defence can be sufficiently counterbalanced to ensure a fair trial.

The Court also made it clear that an earlier provision in the UK that allowed the prosecution (as opposed to the Trial judge) to make the decision as to whether evidence should be disclosed was incompatible with Article 6 of the Convention.

The present practice in both jurisdictions:

Intercept material as evidence

As to use of intercept evidence in this jurisdiction, while the 1993 Act does not specifically prohibit it, there is a long – standing practice not to use it. In the UK 2000 RIPA Act specifically bars any evidence in court, or any question, assertion or disclosure in legal proceedings which results from warranted interception or which would reveal that it had taken place. As already noted above, this matter has been examined in the UK where the Privy Council agreed with the principle that intercept material as evidence should be used in England and Wales and it concluded that a robust legal rules in an appropriate statute, compatible with the ECHR and based on a specially adapted PII model. No change is recommended in the case of Northern Ireland – the stringent disclosure rules there due to the use of non-jury trials – being an important consideration. No change is recommended either in the case of Scotland’s existing PII model of disclosure as the law there has been recently reviewed and public consultations are currently underway.

Material from covert surveillance as evidence.

In our case the operations and practices in this area are not regulated by law and there are no statutory provisions applicable. Up to now, and even before the ECHR ever became an issue, there has been no suggestion that the information gained should be used in evidence. This policy seems to have been based on the same grounds which applied in the case of intercept evidence – that it was better not to open up the prospect of how such information was being obtained, technologically and operationally.

The use of this material in the UK has been permissible since the 1997 Police Act and the general disclosure provisions in the Criminal Procedure and Investigations Act, 1996 and the common law rules of Crown Privilege as adapted by the PII system.

Matters for decision:

Should information obtained by secret surveillance methods be potentially admissible in evidence in certain cases as deemed necessary by the Garda Síochána?

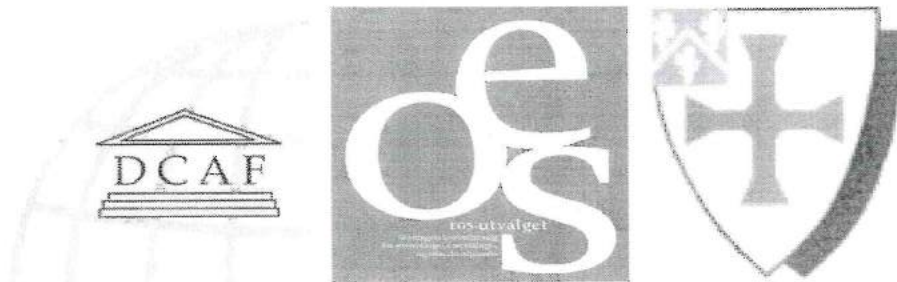
If so, should special rules be put in place for disclosure to the defence of exculpatory material, subject to Public Interest Immunity. Special rules would also be necessary to address any defence challenges to the admissibility of material where sensitive technical/operational information was relevant.

Should provision be made to allow the Gardaí to conduct their operations according to the level of seriousness believed to be involved. In a potentially serious case they would record and retain all the product of the surveillance. In a less serious case they would handle the material differently.

Should a similar change be made in the case of intercept material ?

In summary:

- There are no insurmountable problems over the use of material obtained through covert surveillance in evidence.
- At the very least it would appear that the existing undeveloped common law rules on disclosure in criminal cases would have to be up-dated in statutory form to deal specifically with these cases. Any legislation would have to provide for -
 - a) third party adjudication (possibly the trial Judge) rules on the identification and disclosure of material that is (i) exculpatory and/or (ii) otherwise relevant as the defence may specify,
 - b) refusal of disclosure of information or material which would be contrary to the public interest on the grounds that it might harm or compromise the operational efficiency of the Gardaí to combat terrorism or serious crime, and
 - c) rules to discourage general fishing expeditions by the defence
- However, the reality is that once this type of evidence is introduced, it will become the norm for challenges and applications to be made in all cases. Regard must also be had to the fact that the balance will always be tilted towards disclosure.



Geneva Centre for the Democratic Control of Armed Forces (DCAF)
The Norwegian Parliamentary Intelligence Oversight Committee
Human Rights Centre, Department of Law, University of Durham

THE EUROPEAN COURT OF HUMAN RIGHTS AND INTELLIGENCE ACCOUNTABILITY

Professor Dr. Iain Cameron
Professor in Public International Law, Faculty of Law, University of
Uppsala, Uppsala, Sweden
Cameron@jur.uu.se

Summary of Paper

Oslo, Norway, September 2003

Conference Papers

Conference Papers constitute studies designed to promote reflection and discussion on civil-military relations and issues of democratic control over the defence and security sector. The publication of these documents is unedited and unreviewed.

The views and opinions expressed are those of the author(s) and do not necessarily reflect those of the organisations involved in the conference.

Conference Papers are not for quotation without permission from the author(s) and the Geneva Centre for the Democratic Control of Armed Forces, The Norwegian Parliamentary Intelligence Oversight Committee and the Human Rights Centre, Department of Law, University of Durham.

THE EUROPEAN COURT OF HUMAN RIGHTS AND INTELLIGENCE ACCOUNTABILITY¹

Iain Cameron

Summary of Paper

My paper examines briefly the case law of the European Court of Human Rights (ECtHR), and the now-defunct the European Commission on Human Rights) dealing with national security issues, and assesses the value of this case law as regards the work of devising European principles of accountability for the security and intelligence services. Certain of the rights provided for in the Convention contain an express clause permitting a state to limit the right in question on the basis of "national security", but national security can be relevant, in one way or another, to all the rights in the Convention.

The Convention does not employ the concept of accountability directly: instead the Court has examined systems of accountability as indirect components of the requirements that a limitation on human rights be "prescribed by law", "necessary in a democratic society" and accompanied by "effective remedies" at the national level. The main Convention article which has given rise to accountability discussions is Article 8, as regards the protection of privacy, and in relation to the specific issues of security surveillance and security records/screening. The ECtHR has also delivered important judgments relating to the provision of judicial remedies for deportations on security grounds and security decisions affecting "civil rights".

The Convention case law can be divided into two general periods, pre-1990 and post-1990, corresponding broadly with the end of the cold war. During the first period, the Court delivered a number of landmark judgments, in particular, *Klass and Others v. FRG* and *Leander v. Sweden*, establishing basic, though hardly onerous, principles of accountability. The Court also laid down certain useful procedural safeguards as

¹ Summary of Paper prepared for the Workshop on "*Making Intelligence Accountable*", held 19-20 September 2003 in Oslo, Norway. The Workshop was organised by the Geneva Centre for Democratic Control of Armed Forces (Switzerland), the Intelligence Oversight Committee of the Norwegian Parliament and the Human Rights Centre, Department of Law of the University of Durham (UK).

regards interception of communications, e.g. in the *Kruslin v. France*, *Hewitt and Harman v. UK* and *V. et al v. Netherlands* cases. However, during this period, the case law is largely characterized by too much respect for state arguments, and too much reliance on the supposed efficacy of national control mechanisms, later shown to be deficient (e.g. the *M. S. and P. S. v. Switzerland*, *L. v. Norway* and *Leander v. Sweden* cases).

During the second period, the picture changes (although examples can still be found of bad decisions on the merits, e.g. *Christie v. UK* and *Kalac v. Turkey*). Increased scepticism towards government claims as to the necessity for interferences is evident in a number of cases, e.g. *Observer and Guardian v. UK*, *Bluf v. Netherlands*, *Vogt v. Germany* and as regards government claims that its agents are not responsible for interferences with human rights (e.g. *Tsavachidis v. Greece*). The margin of appreciation in national security issues is no longer uniformly wide. In some matters, the Court states explicitly that there is no margin at all (e.g. *Chahal v. UK*, as regards Article 3). In other areas, most notably Article 6, the Court has significantly limited the margin, explicitly or implicitly applying a "least intrusive means" test (e.g. *Tinnelly and McElduff v. UK*). The Court has maintained, and strengthened, its standards relating to quality of law (*Kopp v. Switzerland*, *Lambert v. France*, *Amman v. Switzerland*, *Rotaru v. Romania*). Even as regards the question of effective remedies, the Convention organs have, at least at times, displayed more scepticism regarding government claims (e.g. *Chahal v. UK*).

The Convention is one of the few common standards applicable to all European states, and as such is invaluable as a starting point for devising common principles of accountability. The main value of the Convention in this area has been in setting minimum levels of foreseeability as regards legal authority to engage in secret surveillance and security filing/screening. However, the minimum nature of the Convention protection, the margin of appreciation, the indirect nature of the review of accountability, the accident of litigation and the restricted competence and legitimacy of the ECtHR mean that the Convention has limited potential to be more than a general platform on which to elaborate more detailed pan-European principles of accountability.



Geneva Centre for the Democratic Control of Armed Forces (DCAF)

rue de Chantepoulet 11, P.O. Box 1360, CH-1211
Geneva 1, Switzerland
Tel: 00 41 22 741 77 00
Fax: 00 41 22 741 77 05
E-mail: h.born@dcaf.ch
Website: <http://www.dcaf.ch>



The Norwegian Parliamentary Intelligence Oversight Committee

Stortinget, 0026 Oslo, Norway
Nedre Vollgt. 5-7
Tel: 00 23 31 09 30
Fax: 00 23 31 09 40
Email: post@eos-utvalget.no
Website: <http://www.eos-utvalget.no>



**Human Rights Centre, Department of Law,
University of Durham**

50 North Bailey, Durham DH1 3ET, United Kingdom
Phone: 00 44 191 374 2035
Fax: 00 44 191 374 2044
Email: ian.leigh@durham.ac.uk
Website: <http://www.dur.ac.uk/Law>

12

XXIIIrd International Conference of Data Protection Commissioners
Paris, 24th - 26th September 2001

**SUMMARY OF THE PAPER READ BY MARCO CAPPATO, EUROPEAN DEPUTY
ON THE " BONINO LIST " AND RAPPOREUR TO THE EUROPEAN PARLIAMENT
ON THE PROTECTION OF PRIVACY IN ELECTRONIC COMMUNICATIONS**

INTRODUCTION

In the Klass Judgement dated 1978, the European Court of Human Rights wrote :

" 49. ... the Court notes that the national legislator enjoys a certain discretionary power (in the choice of the methods used by surveillance systems). Nevertheless, the Court makes it clear that this does not give the member States unlimited latitude in imposing secret surveillance methods on the people who are subject to their jurisdiction. Conscious of the danger inherent in such a law of undermining or even destroying democracy on the pretext of defending it, it confirms that they may not take just any measures they think fit in the name of the fight against espionage or terrorism. "

These words express the risks that our society, our States and our citizens currently run and the limits which a law-abiding State may not exceed. The ferocious and bloody terrorist attacks which struck the United States on 11th September last have encouraged some people to demand " exceptional " laws. In Italy, we have good knowledge of the " exceptional " laws on organised crime and terrorism which are rooted firmly in the penal code (which is the code we inherited from Fascism) and which have also been exported to other countries.

Many people repeatedly say nowadays that we have to sacrifice some of our liberty to gain increased security and that in a time of insecurity exceptional measures are needed. This does not upset me when this concerns controls at airports or when going through customs, however I am opposed to proposals from the State which aim to install permanent systems of access to the private life of citizens.

THE EUROPEAN UNION

The proposed directive from the European Commission on the protection of privacy in electronic communication systems - which modifies a directive dated 1997 on the same subject in the light of new technological developments and as part of a drive to liberalise the telecommunications sector - is currently being examined by the European Parliament and the Council. Certain Ministers of Telecommunications, encouraged by their colleagues in the Home Office and Police forces, want to modify the directive in that part which imposes the deletion of data relating to telephone traffic (the number making the call, the number called, the duration of the communication and the time the communication started and ended, etc.) and the localising of a mobile

phone once the processing of this data for invoicing has been completed. Certain governments within the Council wish to introduce these modifications in order to be able to impose on communications service providers the duty to retain this data for longer periods which may extend up to 7 years, in order to enable police forces, following legal authorisation, to search for the data required to track down criminals and to use it as evidence.

On this point, it should be remembered that this " external " communication data is often treated in the same way as the contents of the communication itself, as Italian case law, for example, has done ; the Italian Supreme Court in 1998 judged that traffic data cannot be used as evidence in a trial without the authorisation of the legal authorities. Therefore the retention of this data - which is one of the phases of processing - whether it is carried out by the State or by the service provider, and since it can be assimilated to the recording of the content of a conversation, must be considered as an interception of the communication. The idea circulating within the Council would therefore aim to achieve the installation of a wide ranging surveillance system.

There is a second consideration to be taken into account, an economic one : the obligation of retaining data on traffic for seven years would represent a significant cost for service providers and this would have economic consequences for subscribers and users. For example, this factor has scuppered the plans of the government of the United Kingdom to establish a State data bank.

Although the Council is moving toward the strengthening of cyber surveillance, the Commission on Liberties and Citizen's Rights unanimously supported my amendments which aimed to introduce into the directive an explicit reference to the jurisprudence of the European Court of Human Rights. The approved text noted :

(Art. 15, para.1) : " The Member States may take legislative measures with the aim of limiting the effect of the rights and obligations provided for in Articles 5 and 6, Article 8, paragraphs 1 to 4, and Article 9 of this directive when this limitation constitutes, *in a democratic society*, a measure which is necessary, *appropriate, proportional and limited in time* to safeguard the security of the State, its defence, public safety, the prevention, search for, detection and prosecution of penal infringements or the unauthorised use of the electronic communications system, as provided for in Article 13, paragraph 1, of the directive 95/46/CE. *These measures must be totally exceptional, based on a specific law which is understandable by the general public and authorised by the legal or competent authorities in specific cases. By virtue of the European Convention on Human Rights and in accordance with the judgements handed down by the European Court of Human Rights, any form of general or exploratory electronic surveillance carried out on a wide scale is forbidden* " .

Following this vote, my Report was sent back to the commission after a vote in plenary session which was highly controversial, in particular on the question of the opt-in or opt-out, on unsolicited electronic commercial communications. As a result, the proposals

of the European Parliament on the protection of private life will have to be discussed once again in the months to come.

Personally, I am going to maintain my position, and not only with regard to a question of fundamentals but also one of method, which affects all of the decisions which the European Union is in the process of taking. On subjects as sensitive as this, we cannot accept a method that is fundamentally undemocratic in the European Union, in particular in connection with the question of cooperation between police forces and legal procedures. The Council discusses and takes decisions in secret. Europol, Schengen, Enfopol and Eurojust are outside the control of any democratic and legal body. Following the terrorist attack in the USA, any resistance to the strengthening of these instruments appears to have been overcome, in particular nearly everybody seems to agree with Europol's operational mandate but the question of the power of Parliament and of the Court has not been raised.

CYBER SECURITY OR CYBER DEMOCRACY : WHICH HAS PRIORITY ?

Obviously, after what has taken place in the United States, all pronouncements are centred on the use of computers by criminal organisations and States. The request for citizens' security to be improved cannot remain unanswered. The route which, for the moment, we have decided to take is that of strengthening the mechanisms of State controls. However, if we are able to accept a new balance between liberty and security, we certainly cannot abandon our principles and the fundamental liberties which characterise democratic and law abiding States in the name of security. In particular, we must oppose all those who take advantage of the situation to impose, like real jackals after power, repressive and even violent policies (even the declarations issued by Putin, who draws a parallel between the violence suffered by the USA and that which Russia "may be suffering" in Chechnya, where in reality he has imported war and terror).

CONSIDERATIONS AND PROPOSALS

* Secret service specialists are almost unanimous in emphasising that the limits of " intelligence " mainly lie in a strategy that is too oriented toward work at a distance and technology, especially the interception of data, and too little based on work carried out in the field with flesh and blood agents. The reason for this strategy is only too easily understood. It takes account of the human and economic costs of direct action. If this strategy on its own has failed, it is perhaps necessary to support it with other measures, with priority given to work in the field.

* Organised criminals are not going to stop when faced with security systems designed to control the general public ; they have the means to use sophisticated systems. On the other hand, we cannot accept that the person monitored, the " enemy ", becomes a simple citizen who surfs on the Net or who makes a telephone call.

* The systems for protecting private life, such as cryptology, may be very useful not only for criminals but also for protecting ourselves from criminals.

* We must design and produce a democratic counter-offensive to disseminate knowledge together with the instruments to help citizens to exercise their power. It is not only a question of protecting citizens (privacy), or fighting criminals (cyber crime), but also and above all of strengthening citizens through new technologies :

- on line democracy : the " on line " transmission of all the public events in our democracies ; the possibility of carrying out all types of " public " acts via the Internet (this is what the draft laws based on popular initiatives are asking for and for which Italian radicals are in the process of gathering signatures)
- the dissemination of information : Radio " Voice of Europe " ; to fight the generators of propaganda with counter-information.
- to overcome censorship, the filters that block the network ; freedom of expression must be included as a condition in international agreements.

Marco Cappato